UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE OKTA, INC. SECURITIES LITIGATION,

Case No. 22-cv-02990-SI

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTION TO DISMISS

Re: Dkt. No. 56

On March 17, 2023, the Court held a hearing on defendants' motion to dismiss the amended complaint. For the reasons set forth below, the Court GRANTS IN PART and DENIES IN PART the motion, and GRANTS Lead Plaintiff leave to amend. Any amended complaint shall be filed **by April 28, 2023.**

INTRODUCTION

This securities fraud case is brought by Lead Plaintiff Nebraska Investment Council, on behalf of itself and a putative class of those who purchased the publicly traded Class A common stock of Okta, Inc. ("Okta") during the period from September 1, 2021, through September 1, 2022, inclusive ("Class Period"). Dkt. No. 48 ("AC") at 1.[1] This action arises from two main events and their aftermath: Okta's acquisition of Auth0, Inc. ("Auth0") in May 2021, and a data security

[1] References to the complaint are to the Amended Class Action Complaint, filed October 13, 2022, at Docket No. 48. For purposes of this motion to dismiss, the Court treats as true Lead Plaintiff's allegations in the complaint and construes these allegations in the light most favorable to Lead Plaintiff, the nonmoving party. *See Parks Sch. of Bus., Inc. v. Symington*, 51 F.3d 1480, 1484 (9th Cir. 1995).

incident that occurred in January 2022 but that was not disclosed until late March 2022.

Defendant Okta is a data security company that "provides identity and access management ('IAM') software that helps companies secure user authentication into applications, and for developers to build identity controls into applications, website web services, and devices. Okta primarily markets the Okta Identity Cloud as a one-stop solution that provides data security for an organization's workforce." *Id.* ¶¶ 2–3. Okta is a "'growth company,' *i.e.*, a company that prioritizes growth over profits." *Id.* ¶ 4. The complaint alleges that Okta has yet to report any net income since its initial public offering in 2017. *Id.* ¶ 51. Also named as defendants in this case are Okta's Chief Executive Officer and Co-Founder Todd McKinnon; current Chief Financial Officer Brett Tighe; and current Executive Vice Chairman, Chief Operating Officer, and Co-Founder Frederic Kerrest (collectively, the "individual defendants"). *Id.* at 1.

Lead Plaintiff alleges that defendants made numerous false and misleading statements and omissions in filings with the Securities and Exchange Commission ("SEC"); in press releases and in interviews with the media; at technology conferences; and during quarterly investor calls throughout the Class Period.

Defendants move to dismiss the complaint, asserting that Okta consistently warned investors of the challenges it faced with the acquisition of Auth0 and the integration of its sales team. Dkt. No. 56 ("Mot.") at 1. Defendants also argue that Lead Plaintiff misapprehends the January 2022 security incident, and that hackers were unsuccessful in actually breaching Okta's or its customers' systems, and that Okta "promptly reported everything it knew about the intrusion[.]" *Id.* Defendants contend, *inter alia*, that none of the statements challenged were false or misleading when made, that Lead Plaintiff has not pled fraud with particularity, and that many of the challenged statements are inactionable puffery, forward-looking, or opinions. Defendants further argue that Lead Plaintiff fails to plead that the individual defendants acted with the requisite scienter.

BACKGROUND

I. Acquisition of Auth0 in May 2021 and Resulting Problems

On March 3, 2021, prior to the start of the Class Period, Okta announced that it would acquire

Auth0 in a stock transaction valued at approximately $6.5 billion. AC ¶ 58. Auth0 "provided customer identity and access management ('CIAM') software, as opposed [to] the IAM software that Okta primarily provided for an employer's workforce." *Id.* ¶ 5. Additionally, where Okta focuses "on pre-built, pre-configured solutions[,] . . . Auth0 is more focused on purpose-built application developers." *Id.* ¶ 59. In a press release, Okta explained that the Auth0 acquisition would "complement Okta's growth in the CIAM market." *Id.* ¶ 58.

On May 3, 2021, Okta announced the successful completion of the Auth0 acquisition. *Id.* ¶ 61. Plaintiff alleges, however, that "soon after the close of the acquisition, Okta began to experience severe problems with the integration of Auth0" but failed to disclose these problems to investors. *See id.* ¶ 8. According to CW2, a former Auth0-turned-Okta Senior Vice President, "the integration process began as promising, but ultimately 'did not go well at all' and was a 'complete nightmare.'" *Id.* ¶¶ 39, 78.

These problems primarily took the form of employee attrition and difficulty integrating the sales teams. The complaint alleges that "[i]mmediately after the acquisition of Auth0, Okta began to shed senior employees." *Id.* ¶ 63. According to CW4, a former Account Executive, "Auth0 employees started to leave Okta 'not long after May or June' 2021." *Id.* ¶¶ 41, 66. Around August 2021, former Auth0 CEO (now Okta's President of Customer Identity) Eugenio Pace announced in an internal letter that senior leadership was leaving the company. *Id.* ¶ 65 & n.13. Auth0 executives who departed around this time included the Chief Legal Officer, the Chief Human Resources Officer, and the Chief Financial Officer. *Id.* Auth0's former Chief Revenue Officer decided to stay at Okta for a few months following the acquisition but "made it clear that he was leaving the company." *Id.* ¶ 65. CW5, an Account Executive during the Class Period, stated that Okta's Chief Revenue Officer (Steve Rowland) and the new President of Worldwide Field Operations (Susan St. Ledger) "'pushed out' all of the 'founding fathers' of Okta as well as other employees that helped build the Company—approximately 75-80% of the VPs and SVPs." *Id.* ¶¶ 42, 67, 80. CW6, a Senior Solutions Engineer employed by Okta from February 2019 through December 2021, described a "'mass exodus' of salespeople – both Okta and Auth0 employees – after Auth0 was acquired, around fall 2021." *Id.* ¶¶ 43, 68.

On September 1, 2021, the first day of the Class Period, Defendant McKinnon announced in an earnings call that the company was accelerating the timeline to unify the Okta and Auth0 sales teams, moving the integration up to the start of the new fiscal year in February 2022. *Id.* ¶ 73. McKinnon stated:

> We've made the decision to accelerate the timeline for integrating the sales organizations under Susan St. Ledger's leadership to the beginning of the new fiscal year in February. This move will allow the unified sales team to sell both platforms and benefits customers by providing more options to meet their unique use cases. . . .

Id.

The complaint alleges that "[a]s the Class Period progressed and Auth0 employees continued to exit the Company, Okta created and adopted an integration plan." *Id.* ¶ 77. According to CW2, "the first phase of the integration plan originally involved the integration of the go-to-market (GTM) teams at each company (this included the sales and marketing teams), which was set to occur on February 1, 2022 . . . ." *Id.* ¶ 78. CW2 stated that this integration plan called for retaining 200 to 300 Auth0 employees as "specialists" who would train and educate Okta employees on Auth0 products for approximately one year. *Id.* ¶¶ 79, 81. Auth0 employees would continue to sell Auth0 products, while Okta employees would continue selling Okta products, "with additional sales staff brought on to help meet goals." *Id.* ¶ 79. CW2 stated that both Okta and Auth0 senior executives signed off on the integration plan and that weekly calls occurred throughout the planning period. *Id.* ¶ 80.

In late 2021, according to CW2, Okta's "finance team determined there was 'no way' that the integration plan was 'humanly possible' for FY2024 and 'completely shut it . . . down.'"[2] *Id.* ¶ 81. Now, the Auth0 sales employees would be "generalists" rather than specialists, and Okta and Auth0 employees would be expected to sell each other's products, despite having no knowledge of or training on each other's products. *Id.* ¶¶ 81–82. "CW2 recalled being informed of the decision to scrap the integration plan around December 2021, but employees were not informed until several

[2] It is unclear whether the reference in the complaint to FY2024 is a typo, as the allegations state that the integration plan was to go into effect at the start of fiscal year 2023.

weeks later in approximately mid-January 2022, two weeks before the integration was supposed to go into effect." *Id.* ¶ 83.

Meanwhile, Okta publicly touted the success of its acquisition of Auth0. In a press release issued September 1, 2021, Defendant McKinnon is quoted as stating, "In our first quarter as a combined company with Auth0, we're off to a fantastic start." *Id.* ¶¶ 71, 134. In an earnings call that same day, McKinnon stated, "It's been less than four months since we closed the acquisition of Auth0, but we've already made a lot of progress and learned quite a bit. . . . [W]hen you think about us plus Auth0, it is going very well." *Id.* ¶¶ 72, 135. A few weeks later, at the Piper Sandler Virtual Global Technology Conference, Defendant Kerrest stated, "So the integration has gone very well. We're about 4 months in. We're pretty good at execution. So we had some pretty good goals for ourselves, but I think we've been beating even those, which is great." *Id.* ¶ 140. Likewise, on September 15, 2021, Defendant McKinnon stated at the Citi Global Virtual Technology Conference, "We're benefiting a lot on that from our -- we have the acquisition of Auth0, we completed back in May. We're really getting into the integration now." *Id.* ¶ 142. Plaintiff alleges that these statements were false and misleading because defendants knowingly or recklessly omitted the material fact that the company had already lost senior Auth0 and key Okta employees who were critical to the success of the integration. *Id.* ¶¶ 137, 141.

Plaintiff also contends that Okta's risk disclosures filed with the SEC during the Class Period were false and misleading. The risk disclosures all contained the following statements:

> ***The acquisition of Auth0 (the "Acquisition") could cause disruptions to our business or business relationships, which could have an adverse impact on results of operations. . . .***
>
> **We may not realize potential benefits from the Acquisition because of difficulties related to integration, the achievement of synergies, and other challenges.**
>
> Prior to the consummation of the Acquisition, we and Auth0 operated independently, and there can be no assurances that our businesses can be combined in a manner that allows for the achievement of substantial benefits. Any integration process may require significant time and resources, and we may not be able to manage the process successfully as our ability to acquire and integrate larger or more complex companies, products or technologies in a successful manner is unproven. If we are not able to successfully integrate Auth0's businesses with ours or pursue our customer and product strategy

> successfully, the anticipated benefits of the Acquisition may not be realized fully or may take longer than expected to be realized. ***Further, it is possible that there could be a loss of our and/or Auth0's key employees and customers, disruption of either company's or both companies' ongoing businesses or unexpected issues, higher than expected costs and an overall post-completion process that takes longer than originally anticipated.***

Id. ¶¶ 138 (Form 10-Q dated Sept. 2, 2021), 153 (Form 10-Q dated Dec. 2, 2021) (emphases in complaint); *see also id.* ¶¶ 159 (Form 10-K dated Mar. 7, 2021), 165 (Form 10-Q dated June 3, 2022).[3] Lead Plaintiff alleges that "[t]hese risk disclosures were false and misleading because Defendants knew or recklessly disregarded that these risks had already materialized. Specifically, Defendants knew or recklessly disregarded the fact that senior Auth0 and key Okta employees had already left the Company." *Id.* ¶ 139; *see also id.* ¶¶ 154, 160, 166.

II. Security Incident in January 2022

According to the complaint, Okta, which prides itself on making data security a priority, "was not properly securing its administrative tools for monitoring customer tenants."[4] AC ¶¶ 97–98. CW6 explained that Okta had a "SuperUser tool" that "provided access to any customer in any Okta tenant anywhere in the world" and which "allowed pre-sale engineers and customer support employees to control and monitor customer tenants." *Id.* ¶ 98. However, "there was no formal request or vetting process for becoming a SuperUser." *Id.* ¶ 99. According to CW6, the newer and less experienced managers in the company handed out SuperUser access "like candy." *Id.* The complaint states that "CW6 went on to suggest that the SuperUser tool should have been more closely guarded against hackers[,]" such as by restricting employees from accessing the tool from their home laptops or through tighter controls on home laptops themselves. *Id.* ¶ 100. CW7 similarly "advised that it seemed too easy for anyone to access these administrative tools." *Id.* ¶ 102. According to CW7, there "wasn't much of a vetting process" to become a SuperUser, and the SuperUser tool required no additional training or security measures. *Id.*

[3] Lead Plaintiff explains that the statements highlighted in bold and italics in the complaint are those that Lead Plaintiff alleges were false or misleading. AC ¶ 133.

[4] "Tenants" in this context are comparable to "virtual servers" that Okta customer support personnel had access to for troubleshooting and monitoring purposes. AC ¶ 98 n.16.

The complaint additionally alleges that "Okta failed to require third parties, such as sub-processors and Solutions Engineers, to comply with the security requirements that are fundamental to Okta's business." *Id.* ¶ 103. "For example, Okta adopted, and strongly recommended that its customers adopt, a 'Zero Trust' security architecture." *Id.* "Zero Trust" meant that security did not operate on the assumption that there was a "trusted" internal network and an "untrusted" external network but that Okta would "securely enable access for the various users . . . regardless of their location, device or network." *Id.*

On January 21, 2022, hackers known as LAPSUS$ "were able to access Okta resources after they compromised one of the Company's third-party support vendors[.]" *Id.* ¶ 104. According to the complaint, the hackers were "able to access Okta resources to view information from the Company's active customer tenants. However, . . . notwithstanding their knowledge of the data breach, Defendants failed to disclose the January 2022 Breach for another two months." *Id.*

On March 7, 2022, Okta filed its Form 10-K for fiscal year 2022 with the SEC. *Id.* ¶ 159. In it, Okta provided the following risk language related to data security:

> ***Security is a mission-critical issue for Okta and for our customers.*** Our approach to security spans day-to-day operational practices from the design and development of our software to how customer data is segmented and secured within our multi-tenant platform. ***We ensure that access to our platform is securely delegated across an organization. . . .***
>
> ***The Okta Identity Cloud is monitored not only at the infrastructure level but also at the application and third-party integration level. Synthetic transaction monitoring allows our technical operations team to detect and resolve issues proactively. . . .***
>
> . . . A summary of our risks includes, but is not limited to, the following: . . .
>
> - ***An application, data security or network incident may allow unauthorized access to our systems or data or our customers' data, disable access to our service, harm our reputation, create additional liability and adversely impact our financial results.***

Id. Plaintiff alleges these statements "were materially false and misleading because these risks had already materialized. Specifically, Okta had experienced the January 2022 Breach due to unsecured administrative tools used for monitoring cloud tenants and the failure to require sub-processors to

comply with Okta's fundamental security requirements." *Id.* ¶ 160.

On March 21, 2022, "LAPSUS$ posted screenshots on their telegram channel showing what they claimed was Okta's internal company environment." *Id.* ¶ 105. On March 22, 2022, at 4:23 a.m., Defendant McKinnon posted the following statement on his Twitter account:

> In late January 2022, Okta detected an attempt to compromise the account of a third party customer support engineer working for one of our subprocessors. The matter was investigated and contained by the subprocessor. (1 of 2)
>
> We believe the screenshots shared online are connected to this January event. Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January. (2 of 2)

Id. ¶ 106. Okta's stock price fell $2.98 per share, or 1.76%, to close at $166.43 on March 22, 2022. *Id.* ¶ 107.

Later in the day on March 22, Okta's Chief Security Officer David Bradbury issued several blog posts on the security incident. According to the complaint, "[i]n this post, Bradbury admitted that Okta first detected the January 2022 Breach in January." *Id.* ¶ 108. In a follow-up post, Bradbury stated that "approximately 2.5%" of Okta's customers had "potentially been impacted and whose data may have been viewed or acted upon."[5] *Id.* Raymond James downgraded Okta from "strong buy" to "market perform," stating, "[w]hile partners were willing to trust Okta's track record, the handling of this latest security incident adds to our mounting concerns." *Id.* ¶ 109. As a result of the Raymond James downgrade and Okta's update after the close of market, Okta's stock price fell $17.88 per share, or 10.74%, to close at $148.55 on March 23, 2022. *Id.* ¶ 110. The complaint alleges, "On March 25, 2022, Okta acknowledged that it sat on this information for almost two months before stating, 'We want to acknowledge that we made a mistake.'" *Id.* ¶ 111.

III. Customer Responses

Several of the confidential witnesses described the fallout after the security incident was revealed. According to CW3, a Corporate Account Executive whose territory covered half of

[5] A CNN article published March 23, 2022, estimated that because Okta had over 15,000 customers, 2.5% would equate to hundreds of clients potentially impacted. AC ¶ 108.

Dallas, "the Company was saying that they were losing sales because of the breach, and CW3 noted that the breach did come up with every customer she spoke with, and the Company distributed 'talking points' to employees on how to 'downplay' the breach. CW3 described the breach as 'one of many hurdles' that were necessary to clear to achieve a successful sale." AC ¶ 113. "Similarly, CW4 recalled that prospective customers were deciding against doing deals with Okta after the breach." *Id.* ¶ 114. CW4 was an Account Executive based in Europe who was employed by the company until the first quarter of fiscal year 2023. *Id.* ¶ 41. CW8, a Senior Account Executive whose clients were based in the New York City area, also "advised that Okta customers reacted negatively to the data breach that Okta disclosed in March 2022." *Id.* ¶¶ 45, 115. Following the breach, Okta customers were unwilling to expand their contracts and "express[ed] that they were no longer comfortable spending additional money with Okta[.]" *Id.* ¶ 115. The negative customer reaction impacted CW8's ability to meet quotas; although "CW8 could not quantify the amount of lost business, . . . she suggested it might have been 'tens of thousands of dollars' in lost business." *Id.* This compounded Okta's struggles in the wake of the faltering Auth0 integration.

On June 8, 2022, Defendant McKinnon gave a CNBC interview, where he discussed customer reaction to the security incident and what the company had done to repair those relationships. During the interview, McKinnon stated:

> And anytime there's any kind of hack, whether it's to a third party or what any kind of talk of a breach, there's a lot of concerns in the [sic] in the customer base because this is about trust. So, the first thing we did is we had these conversations. We talked to over 1000 customers face to face over, [sic] over video and had these conversations. I personally talked [sic] over 400. ***And got a ton of feedback about what we could do better, how we could make sure that our support environment was not insecure, to make sure that we communicate better, to make sure that we are instill [sic] this trust. At the end of the [sic], I think we've been able to do that.***
>
> . . .
>
> ***We're committed to making this a $4 billion a year company by fiscal year, fiscal year 26. So, that's, that's coming up quickly. So, we have to invest to grow to that scale and we've always done it with a balance of efficiency.*** We've always made sure that our, that our growth rate and our [sic] and our cash flow generation was balanced towards that goal. ***So, we think we're drawing the right balance to capture this market opportunity.*** And I think over time you're going to see a very highly scaled profitable company that's going to help customers and capitalize on this big market opportunity.

Id. ¶¶ 167–68 (underlined [sic]'s added by the Court).

IV. Disclosure of Attrition and Integration Challenges

On August 31, 2022, after the close of the trading day, Okta held its second quarter earnings call. AC ¶ 126. Lead Plaintiff alleges that it was on this call that "Defendants finally disclosed issues related to the integration of Auth0." *Id.* Explaining the "mixed" financial results for that quarter, Defendant McKinnon stated, in part:

> **And the third area we examined was impact from the integration of the Okta and Auth0 sales teams, which occurred at the beginning of this fiscal year.** When talking about Auth0, it's important to revisit the strategic rationale of why we acquired Auth0. Individually, Okta and Auth0 were leading identity providers. Together, we offer the most comprehensive identity platform in the market that is unmatched competitively and creates powerful long-term network effects for us and for our customers. Organizations around the globe are looking for scalable and secure ways to digitally interact with our customers. Together with Auth0, we win the customer identity market faster and accelerate our vision of establishing Okta as a primary cloud.
>
> Integrations are always difficult and touch every part of an organization. **While we are making progress, we've experienced heightened attrition within the go-to-market organization as well as some confusion in the field, both of which have impacted our business momentum. In order to improve our performance going forward, we've implemented a number of action items. For starters, we're committed to stem attrition within our go-to-market team. This is a top priority for me and my staff, and we're in lockstep on actions to take. This includes making changes to our organizational structure to better align on our strategy, increased sales training and enablement and also improving the comp structure for the go-to-market team to ensure they feel set up for success.**

Id.

In response to a question about the integration of the Auth0 and Okta sales teams, McKinnon replied:

> Yes, for sure. Thanks for the question. I think there's -- in terms of -- I'll start first with sales organization. The big change on the sales organization was at the beginning of this fiscal year, so Feb 1, and that's where we took the Auth0 sales team that sold as an independent group all through last year for the first three quarters of the -- after the acquisition and we combine them together with the Okta sales team.
>
> And so, **the idea there is that hundreds and hundreds of Okta reps**

> **sell the whole portfolio, Okta plus Auth0. And then the Auth0 reps that came over sold the Okta portfolio and Auth0 portfolio. So that was a really significant step in the integration.** In terms of -- one thing I want to clarify is that Freddy [Kerrest] doesn't manage the sales team.
>
> * * *
>
> **I think the headwinds are really about how do you take those hundreds and hundreds of reps and make them productive selling both customer identity cloud and workforce identity cloud, and there's a couple of things that go into that**. The first thing is that we really have to reach a new buyer for Okta, which is -- Okta traditionally was about CIOs and CISOs. But for customer identity to be successful, we have to reach VPs of technologies, CTOs, all of the chief marketing officers, chief digital officers, the whole suite of C-suite executives that will -- if we win them all and we have an identity platform for all those use cases, we can better achieve our goal of being the primary cloud and the primary piece of their strategic landscape going forward.

Id. ¶ 127.

Defendants McKinnon and Tighe also told investors on the call that Okta was reevaluating its current year billings outlook and its FY26 targets. McKinnon stated:

> Yes, it's a great question. On the first part of your question, ***so the $4 billion FY '26 target, if we're going to achieve that, when we're going to achieve that, we have to have a successful customer identity cloud. And so as we reevaluate in the short-term how to keep that momentum going, I think it's prudent to make sure that we reevaluate that target given the short-term changes that we're optimizing for the customer at a cloud.*** And then -- and we're committed to coming back to everyone on the next earnings call with a very detailed refined version of that -- of those commitments and that target, I think it's very important. So, that's the first thing.
>
> And then on the second thing, the sequence of events here, ***I think, which is important for everyone to understand is that the sales teams were integrated this year. So, it's really 6 months of information and learnings that we have to iterate on this thing.***
>
> It's not -- ***last year, Auth0 ran as a separate sales team, and they had a great year. So, we know there's market fit. We know we can grow this thing. It's just about the integration of the sales teams and what that drove in terms of attrition, and some of the things we've talked about in terms of optimizing how we get that back on track to achieve this strategic imperative***, which is we have to be the winner and the opportunity is tremendous in this long-term customer identity market.

Id. ¶ 128. Defendant Tighe stated:

> . . . We will continue providing a full year billings outlook for FY '23 before discontinuing any reference to billings in FY '24. ***We are lowering our calculated billings outlook for the year by***

> ***approximately $140 million due to the outlook headwinds outlined earlier.*** We now expect calculated billings for FY '23 to be approximately $2.04 billion to $2.05 billion, representing growth of 27% when viewed on a like-for-like basis or 19% on an as-reported basis.
>
> ***Given our near-term outlook, coupled with the uncertainties of the evolving macro environment, we are reevaluating our FY '26 targets at this time.*** Having said that, we will continue to balance growth and profitability, and we look forward to updating you on our long-term outlook on the Q3 earnings call.

Id. ¶ 129.

The complaint states, "On this news, the price of Okta's stock fell dramatically overnight to [sic] $22.25 per share, or ***over 24.3%***, to open at $69.15 on September 1, 2022." *Id.* ¶ 130.

On September 1, 2022, Defendant McKinnon was interviewed on TechCheck, where, according to the complaint, "he reaffirmed that Okta was having issues obtaining new customers." *Id.* ¶ 202. McKinnon stated,

> **Yeah, we have had a little bit of higher-than-average attrition in the sales team and that driving [sic] some of the near-term mixed results. I think when you look at the quarter though I think there are sales people being successful at Okta. We had a record number of $1,000,000 plus deals in the quarter and so on we had great customer retention our net retention percussion which is really emblematic of customer success is 120% plus so there's a lot of success going on but when you think about trying to reach this new buyer and bringing two sales forces together and [*sic*] and sort of trying to broaden that appeal in this C suite of every organization in the world that's challenging in [*sic*] a little bit more challenging than we thought it would be so we're gonna work through those issues can [sic] move forward.** I think on your macro question, we are seeing a little bit of macro change a little bit of lengthening sale cycles but, I think big picture wise that's [*sic*] that's a very small part of our mixed results, and we have a lot of these corrective actions we're taken [sic] in short term are going to yield to a lot of positive momentum in the future.

Id. (underlined [sic]'s added by the Court). The price of Okta's stock fell an additional $8.55 per share that day, or over 12.3%, to close at $60.60 by the close of trading on September 1, 2022. *Id.* ¶ 24.

V. Filing of This Lawsuit

On May 20, 2022, plaintiff City of Miami Fire Fighters' and Police Officers' Retirement Trust filed suit against Okta and five individual defendants regarding the January 2022 data security

incident. Dkt. No. 1 (alleging class period of March 5, 2021, to March 22, 2022, inclusive). On August 26, 2022, the Court appointed Nebraska Investment Council as Lead Plaintiff. Dkt. No. 39. On October 13, 2022, Lead Plaintiff filed an amended class action complaint, which is now the operative complaint, adding allegations regarding the Auth0 integration. *See* Dkt. No. 48. Alleging that defendants committed fraud by making materially false statements and omissions throughout the Class Period, Lead Plaintiff brings this securities fraud claim pursuant to Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5(b) promulgated thereunder by the SEC. Defendants now move to dismiss for failure to state a claim under Federal Rules of Civil Procedure 9(b) and 12(b)(6).

LEGAL STANDARDS

To survive a motion to dismiss brought under Federal Rule of Civil Procedure 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Telesaurus VPC, LLC v. Power*, 623 F.3d 998, 1003 (9th Cir. 2010) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)). When evaluating a motion to dismiss, the Court need not accept as true conclusory allegations, unwarranted deductions of fact, or unreasonable inferences. *In re Gilead Scis. Sec. Litig*., 536 F.3d 1049, 1055 (9th Cir. 2008). Securities fraud class actions must also "meet the higher, exacting pleading standards of Federal Rule of Civil Procedure 9(b) and the Private Securities Litigation Reform Act (PSLRA)." *See Tellabs, Inc. v. Makor Issues & Rights, Ltd*., 551 U.S. 308, 313–14 (2007).

Rule 9(b) requires a party alleging fraud or mistake to "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b). The PSLRA further requires that allegations based on false or misleading statements must also "specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed." 15 U.S.C. § 78u-4(b)(1)(B). Additionally, the complaint must "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind" for "each act or omission." *Id.* § 78u-4(b)(2)(A).

To state a claim under Section 10(b) of the Exchange Act and SEC Rule 10b-5, the complaint must plausibly allege: "(1) a material misrepresentation or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *Weston Family P'ship LLP v. Twitter, Inc.*, 29 F.4th 611, 619 (9th Cir. 2022) (citing *Halliburton Co. v. Erica P. John Fund, Inc.*, 573 U.S. 258, 267 (2014)).

To establish falsity under the first element, the misrepresentation or omission must either "directly contradict what the defendant knew at that time" (i.e., is false) or "omit[ ] material information" (i.e., is misleading). *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1008–09 (9th Cir. 2018). Not all omissions are actionable. *Id.* at 1009. "Disclosure is required . . . only when necessary 'to make . . . statements made, in the light of the circumstances under which they were made, not misleading.'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (quoting 17 CFR § 240.10b–5(b)). For a statement or omission to be misleading, it must "affirmatively create an impression of a state of affairs that differs in a material way from the one that actually exists." *Brody v. Transitional Hosp. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002) (citation omitted). "To fulfill the materiality requirement there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." *Miller v. Thane Int'l, Inc.*, 519 F.3d 879, 889 (9th Cir. 2008) (quoting *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 449 (1976)) (cleaned up).

The "required state of mind" for scienter covers "'intent to deceive, manipulate, or defraud,' [and] also 'deliberate recklessness.'" *Schueneman v. Arena Pharms.*, 840 F.3d 698, 705 (9th Cir. 2016) (citations omitted). To determine whether scienter has been adequately pled, the Court must determine whether "*all* of the facts alleged, taken collectively, give rise to a strong inference of scienter." *Tellabs*, 551 U.S. at 310. Plaintiffs who "seek to hold individuals and a company liable on a securities fraud theory" must "allege scienter with respect to each of the individual defendants." *Oregon Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 607 (9th Cir. 2014).

The Supreme Court's decisions in *Tellabs*, 551 U.S. at 315–18, and *Matrixx Initiatives*, 563

U.S. at 37–49, dictate that courts not co-mingle the inquiries of falsity and scienter. *Glazer Capital Mgmt., L.P. v. Forescout Techs., Inc.*, No. 21-16876, 2023 WL 2532061, at *11 (9th Cir. Mar. 16, 2023). "[T]his means that we do not impute the strong inference standard of scienter to the element of falsity; we do not require a 'strong inference of fraud.' Falsity is subject to a particularity requirement and the *reasonable inference* standard of plausibility set out in *Twombly* and *Iqbal*, and scienter is subject to a particularity requirement and a *strong inference* standard of plausibility." *Id.*

If the Court dismisses a complaint, it must decide whether to grant leave to amend. The Ninth Circuit has "repeatedly held that a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts." *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000) (citations and internal quotation marks omitted).

DISCUSSION

I. Exchange Act Claims

In the analysis that follows, the Court discusses only the disputed elements of Section 10(b): material misrepresentation or omission, and scienter.

A. Employee Attrition and the Auth0 Integration

Lead Plaintiff challenges as false or misleading roughly 15 statements regarding the Auth0 integration. *See* Opp'n at 12 (citing AC ¶¶ 134–36, 138, 140, 142, 150–51, 153, 155–57, 162–63, 165). The Court concludes that these allegations fail to point to a violation of the PSLRA because they suffer from a lack of specificity, particularly with regard to timing, or else they do not give rise to a strong inference of scienter.

1. Statements in September and Early December 2021

First, the complaint lacks particularized detail about the timing of the events that would show that statements made in September and early December 2021 regarding employee attrition and the Auth0 integration were false or misleading when made. The complaint challenges nine statements

that defendants made during that period. *See* Dkt. No. 61 ("Opp'n") at 12 (citing AC ¶¶ 134–36, 138, 140, 142, 150–51, 153). The dates of these alleged misstatements range from September 1, 2021, through December 2, 2021. But the complaint lacks particularized allegations regarding what happened and when. What we know from the complaint is that three Auth0 executives left around August 2021. AC ¶ 65. A fourth executive decided to stay for the first few months after the acquisition but, at some unspecified time, he "made it clear he was leaving the Company." *See id.* CW5 states that Okta's Steve Rowland and Susan St. Ledger "'pushed out' all of the 'founding fathers' of Okta as well as other employees that helped build the Company—approximately 75-80% of the VPs and SVPs," but CW5 does not say who these employees are and when they left.[6] *See id.* ¶¶ 67, 80. CW4 recalls "that Auth0 employees started to leave Okta 'not long after May or June' 2021." *Id.* ¶ 66. The complaint alleges, via CW6, that there was a "mass exodus of salespeople" from both Okta and Auth0 "around fall 2021." *Id.* ¶ 68. According to the complaint, "CW1 also recalled hearing that the board was reviewing attrition figures in light of the companies' cultural differences and was 'very concerned.' CW1 clarified that this probably happened around the fall of 2021." *Id.* ¶ 221. The complaint alleges: "As the Class Period [beginning September 1, 2021,] progressed . . . Okta created and adopted an integration plan" that would go into effect in February 2022. *Id.* ¶¶ 77–78. Then, "late in 2021," Okta's finance team determined there was "no way" the original integration plan was "humanly possible" for FY2024 and shut it down. *Id.* ¶ 81. CW2 found out about the decision to abandon the integration plan "around December 2021," and employees were informed in mid-January 2022, two weeks before the integration would go into effect. *Id.* ¶ 83.

Plaintiff's theory is that the loss of senior Auth0 and key Okta employees, as well as the "mass exodus" of the salesforce, caused Okta to abandon its original integration plan, and thus defendants' statements that the integration was going well were false or misleading. Even taking all of Lead Plaintiff's allegations as true, it appears that the departure of the three Auth0 executives around August 2021 had no impact on the integration plan because, according to plaintiff's own

[6] The complaint states that Defendants McKinnon and Kerrest are "co-founders" of Okta. *See* AC ¶¶ 32, 34. They remain at the company.

chronology of events, the original integration plan wasn't even created and approved until after the start of the Class Period in September 2021, i.e., after these executives had already departed. *See id.* ¶¶ 65, 77. It is further unclear from the timeline whether the "mass exodus" of sales employees occurred prior to any of the statements that Okta made in September and early December 2021.

The vagueness around timing means that plaintiff has failed to state with particularity facts giving rise to a reasonable inference that the statements regarding the Auth0 integration from September and early December 2021 were false or misleading *when made*. The Ninth Circuit recently held as much in *Glazer Capital Management, L.P. v. Forescout Technologies, Inc*. There, the appellate court explained that

> [a]lthough the CWs asserted that numerous layoffs occurred at some point in 2019, these statements are unclear as to the actual timeline at which company-wide layoffs occurred. Plaintiffs' belief that company-wide lay-offs had already begun at the time the statements were made [on March 4, May 9, or August 7, 2019] is simply not supported by the CWs' vague statements that layoffs occurred in 'spring 2019,' 'summer 2019,' or just '2019.'

2023 WL 2532061, at *19 (analyzing allegations on a motion to dismiss). Likewise here, the only statement regarding employee attrition that is tied to a particular time period *after* the original integration plan was created is the statement of CW6 that there was a "mass exodus" of salespeople "around fall 2021."[7] *See* AC ¶ 68. "Around fall 2021" is not sufficiently particularized to render statements made in September and early December 2021 false or misleading when made.

Accordingly, the Court GRANTS, without prejudice, defendants' motion to dismiss, with regard to statements made in September and early December 2021 regarding employee attrition and the Auth0 integration.

2. Earnings Call Statements on March 2 and June 2, 2022

The complaint also alleges misstatements by the individual defendants on quarterly earnings calls on March 2 and June 2, 2022. *See* AC ¶¶ 155–57, 162–63. Plaintiff alleges these were misstatements because the mass exodus of employees meant that Okta could not maintain a team of

[7] The "mass exodus" language is also attributed to CW5, but CW5 does not say which employees were leaving and when. *See* AC ¶ 90.

specialized staff for Auth0 products, and that Okta and Auth0 salespeople did not have the knowledge required to sell each other's products. *Id.* ¶¶ 158, 164.

On March 2, 2022, Defendant Tighe stated,

> My second priority is ensuring that we continue the seamless integration of Auth0 across all facets of the company. Now that the back office and go-to-market teams have been fully integrated, we will continue to refine our systems and processes to ensure that the tremendous growth opportunity we see will be realized. ***We are off to a great start and recognize there is still a lot of work to do.***

Id. ¶ 155.

Defendant Kerrest stated, in response to a question about the sales force integration,

> Yes. We are -- thanks a lot for the question, Jonathan. We are very excited about the integration of Auth0. We're very excited that it's been done in just under a year from where we are because we actually announced the acquisition a year ago tomorrow. As – to start with, I think the most important point is the go-to-market organization, which we unified under Susan's leadership on February 1. You heard Todd talk about one team, which I think is a great position to be in. We've put together a lot of the core systems that we're using to run the business. Those are all running on one platform. ***So we have one pane of glass and good visibility into all that and how it's working. There's a couple more pieces we need to finish up in terms of ticking and tying some of the systems on the back end, but those are just making sure that we're working as one organization going forward.***

Id. ¶ 156.

On the same call, McKinnon stated,

> ***What we're getting is we're getting synergy on the -- really on the sales side. So we have -- all of the Okta reps now can sell all the products. So we increased the capacity. We can -- we increased what they can actually sell. So there's tons of upside from that.*** But Eugenio has a big job to do with the Auth0 product unit, driving that. They just delivered -- you heard the results. They delivered over 80% growth, and we expect them to produce a lot in the year ahead.

Id. ¶ 157.

Three months later, on an earnings call on June 2, 2022, Defendant McKinnon responded to a question regarding the sales integration process as follows:

> . . . We just celebrated the 1-year anniversary of joining forces with Auth0, which is great. And as we've said in the past, the key here is keeping the momentum going in both Okta and Auth0. Both businesses were doing very well, and that's the continued focus. ***We've made a lot of progress as a combined company.*** Many parts of the back office functions were integrated over the course of FY'22,

> which is great. ***And we started Q1 with the combination of go to -- combining the go-to-market organizations.***
>
> I think there's no real finish line when it comes to integrations. But I think we're really focused on addressing this massive customer identity access management market in a way that, frankly, no other vendor can in terms of independence and neutrality, we have the only 2 modern public cloud solutions and certainly no in-house IT can. ***So I think we've made great progress. There's still a little bit to do, but we're in good shape.***

Id. ¶ 162.

On the same call, Defendant Tighe stated:

> ***And any integration or acquisition and integration of 2 companies, the sales integration is one of the biggest milestones there are. And for this integration between Auth0 and Okta, 2 great sales teams being brought together, it's no different, right? It was a great milestone for us. It was a big one for us, and we're pleased with the progress, thus far.***

Id. ¶ 163.

Suspending for the moment the question of *why* Okta scrapped the original integration plan, the complaint alleges with particularity that around December 2021 the company decided to abandon the integration plan it had had in place for months, and that on just two weeks' notice Auth0 and Okta sales employees found out they would sell each other's products while lacking the training to do so. CW2 was Senior Vice President and General Manager of the Americas, who worked for the company from August 2018 until July 2022. *Id.* ¶ 39. CW2 was "intimately involved" in the Auth0 integration, spending "eight hours per day over a period of six or seven months putting together the integration plan." *Id.* CW2 recalled that the original plan involved retaining Auth0 employees for approximately one year, while they continued to sell Auth0 products and train and educate Okta employees on those products. *Id.* ¶¶ 78–79. Meanwhile, Okta employees would continue selling Okta products. *Id.* ¶ 79. However, after Okta scrapped this plan around December 2021, sales employees were given just half a month's notice before they would begin selling each other's products, rather than one year of working together before Okta employees began selling Auth0 products. *See id.* ¶¶ 81–83. According to CW2, neither Okta nor Auth0 employees had knowledge of each other's products and did not receive training or education on each other's products. *Id.* ¶ 92.

Having chosen to publicly tout the integration of the sales team, it was incumbent on defendants "to do so in a manner that wouldn't mislead investors, including disclosing adverse information that cut[] against the positive information." *See Schueneman*, 840 F.3d at 705–06 (quoting *Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 987 (9th Cir. 2008)) (internal quotation marks omitted). For instance, Defendant Kerrest's statement that "[t]here's a couple more pieces we need to finish in terms of ticking and tying some of the systems on the back end" makes it sound like the company was just tying up loose ends, not that they needed to retrain the entire salesforce in the basic functions of their jobs. *See* AC ¶ 155. Defendant Tighe similarly referred to the integration as "seamless" and implied that "[n]ow that the back office and go-to-market teams have been fully integrated," all that remained to do was "refine our systems and processes[,]" which a reasonable investor would not understand to mean retraining hundreds of employees. *See id.* ¶ 155. Defendant McKinnon's statement that they had "increased the capacity" of the sales reps and that there's "tons of upside from that" because "all of the Okta reps now can sell all the products" likewise omits the material fact that the reps were not in fact capable of selling the products because they lacked the knowledge and training to do so. *See id.* ¶ 157.

The Court disagrees with defendants' characterization of these statements as inactionable corporate puffery. "The statements went beyond mere optimism by providing a concrete description" of the sales team integration. *See Glazer Capital Mgmt.*, 2023 WL 2532061, at *15 (cleaned up). Defendants represented that the teams were now "fully integrated," whereas Lead Plaintiff alleges that "neither Okta employees nor Auth0 employees had knowledge of each other's products" at this point. AC ¶¶ 155, 164.

Nor do these allegations suffer from a lack of scienter. Whether or not the newly integrated sales team that Okta touted was in fact trained to sell the products they were tasked to sell, following the $6.5 billion acquisition of Auth0, is of such prominence "that it would be absurd to suggest that top management was unaware of [it]." *See Berson*, 527 F.3d at 989 (citation and internal quotation marks omitted). The Court finds the statements the individual defendants made on the March 2 and June 2, 2022 earnings calls to be actionable under the facts alleged in the complaint and DENIES defendants' motion to dismiss claims based on these statements.

3. Risk Disclosures in March and June 2022

What remains, then, of the Auth0 integration statements are Lead Plaintiff's allegations that Okta's risk disclosures in SEC filings in March and June 2022 were materially false or misleading. In its Form 10-K filed March 7, 2022, and in its Form 10-Q filed June 3, 2022, Okta made the following risk disclosure regarding the acquisition of Auth0:

> ***Further, it is possible that there could be a loss of our and/or Auth0's key employees and customers, disruption of either company's or both companies' ongoing businesses or unexpected issues, higher than expected costs and an overall post-completion process that takes longer than originally anticipated.***

AC ¶¶ 159, 165. Lead Plaintiff alleges that this was materially false or misleading because defendants knew that the risk warned of had already materialized, i.e., that defendants "knew or recklessly disregard the fact that the Company had lost senior Auth0 and key Okta employees, who were critical to the Auth0 integration and that, as a result, the Company could no longer maintain a team of specialized staff for Auth0 products." *Id.* ¶ 154.

a. Misstatements

Although it is a close call, the Court agrees with defendants that the allegations here regarding employee attrition are not sufficiently particularized to meet the pleading threshold of Federal Rule of Civil Procedure 9(b) and the PSLRA.

With regard to the loss of senior executives, as already explained above, the complaint alleges that three Auth0 executives departed before Okta even created the original integration plan, so it cannot be that their departure is what caused the integration plan to fail. The complaint also lacks any allegation that Okta represented that these executives would stay on, or that their departure was not part of the acquisition plan. *See* AC ¶¶ 65, 67. The same is true of the allegation (untethered to any time period) that Okta executives "pushed out" all of the (unnamed) "'founding fathers' of Okta as well as other employees that helped build the Company—approximately 75-80% of the VPs and SVPs." *See id.* ¶ 67. In fact, as we know, two of Okta's co-founders, McKinnon and Kerrest, stayed on in their roles at the company. *See id.* ¶¶ 32, 34.

With regard to the loss of salespeople and Auth0 employees generally, the complaint is not sufficiently specific to raise a reasonable inference that the March and June 2022 risk disclosures were materially false or misleading when made. CW2 explained that Okta intended to retain 200 to 300 Auth0 sales employees and to bring on additional sales staff. *Id.* ¶¶ 79, 81. But the complaint gives no concrete sense of how many employees were lost and on what timeline. For instance, the complaint lacks context for CW1's statement that "only about 15% of the Auth0 employees who moved to Okta during the acquisition are still at the Company," or for CW2's statement that "there are 'very, very few' Auth0 people left." *Id.* ¶¶ 89, 92. Neither of these confidential witnesses specify the time period they are referring to, and both CW1 and CW2 have since left the company. *See id.* ¶¶ 38 (CW1 departed in April 2022), 39 (CW2 departed in July 2022). It is unclear from the allegations whether they meant that there were few Auth0 people left as of the filing of the amended complaint or at some earlier time.

Without more specifics, the Court cannot find that the complaint pleads with particularity that the risk disclosure statements regarding possible employee attrition "affirmatively create[d] an impression of a state of affairs that differ[ed] in a material way from the one that actually exist[ed]." *See Brody*, 280 F.3d at 1006.

b. Scienter

Moreover, the complaint does not allege with particularity what the individual defendants knew regarding employee attrition and when. Although the defendants would certainly have known about the departure of high-level executives, it is not clear when the attrition of line-level sales employees would have risen to the point at which the individual defendants would have found out or would have been reckless in not knowing.

The complaint is silent about the individual defendants' knowledge of employee attrition until the quarterly call on August 31, 2022, when Defendant McKinnon stated, "While we are making progress, we've experienced heightened attrition within the go-to-market organization as well as some confusion in the field, both of which have impacted our business momentum." *See* AC ¶ 194.

This statement does not, as plaintiff argues, provide proof of defendants' earlier scienter. The Ninth Circuit's decision in *Ronconi v. Larkin* is instructive. 253 F.3d 423 (9th Cir. 2001), *abrogated on other grounds as explained in Glazer Capital*, 2023 WL 2532061, at *11. There, the plaintiffs alleged that the defendants' statements attributing low third quarter earnings to post-merger issues amounted to a "later statement by the defendant along the lines of 'I knew it all along.'" *Id.* at 432. The Ninth Circuit disagreed, explaining, "The statement does not support an inference that company insiders knew or with deliberate recklessness disregarded that the problems would be so substantial. . . . [T]he later statement admits only that the below-expectation earnings in the third quarter were a result of the prior integration of the companies' sales force, which concedes no intentional or deliberately reckless falsehood or deception at all." *Id.* Here too, Defendant McKinnon's August 31, 2022 statement attributing mixed financial results in part to "heightened attrition" does not support the inference that the individual defendants acted with intent or deliberate recklessness in issuing the earlier risk disclosures containing general warnings about possible attrition.

Plaintiff also makes an argument for corporate scienter through the knowledge of Okta executives Susan St. Ledger and Steve Rowland. Opp'n at 34 (citing AC ¶¶ 67, 80). Yet the complaint is silent as to what these executives knew regarding attrition of the company's salesforce, other than stating that they were involved in weekly status updates and "signed off on everything" regarding the integration plan. *See* AC ¶ 80.

Even viewing the allegations of the complaint holistically, the Court finds scienter regarding employee attrition lacking. Plaintiff's theory is that the loss of key executives and the mass exodus of salespeople caused defendants to have to abandon their original integration plan. But the complaint does not actually provide details to show this happened. The complaint implies—but does not actually allege with specificity—that the decision in late 2021 to abandon the initial integration plan was *because of* the departure of too many employees. On this, CW2 stated simply that "the finance team determined that there was 'no way' that the integration plan was 'humanly possible' for FY2024 and 'completely shut it [the integration plan] down.'" *Id.* ¶ 81. And although CW2's perspective was that the integration plan "was ripped out at the eleventh hour," the complaint

also states that the reason employees were not notified about the change until mid-January was so as not to disrupt the fiscal year end. *See id.* ¶ 83 (internal quotation marks omitted). This might be a different situation if Okta had told investors it was going to retain specific executives while hiding that those executives had already left or would do so soon. *See Moradpour v. Velodyne Lidar, Inc.*, No. 21-cv-1486-SI, 2022 WL 2391004, at *13–14 (N.D. Cal. July 1, 2022). There are no allegations that Okta told investors that it would retain a certain percentage of its workforce and then hid that it had not met those figures. Nor are there allegations that Okta was secretly plotting to terminate employees while publicly saying they would retain them.

In sum, drawing all reasonable inferences in Lead Plaintiff's favor, what Lead Plaintiff describes is: following the acquisition of Auth0 in May 2021, some executives departed; and over some period of time ("around fall 2021," according to CW6) the company was not able to retain its line-level salesforce; and in December 2021 Okta's finance team pulled the plug on the original sales team integration plan. Then on August 31, 2022, Defendant McKinnon cited "heightened attrition" as one of the factors causing "headwinds" with the integration, which resulted in the company lowering its calculated billings outlook for the year by $140 million and reevaluating its FY26 targets. *See* AC ¶¶ 126–29. These allegations are not sufficiently particularized to create a strong inference that the individual defendants knew or recklessly disregarded material facts regarding employee attrition when they signed off on the risk disclosures on March 7 and June 3, 2022.

That Lead Plaintiff alleges no suspicious stock sales by senior executives also cuts against the inference of scienter, particularly where the complaint is lacking overall in allegations creating a strong inference of scienter as to employee attrition. *Cf. In re Alphabet, Inc. Sec. Litig.*, 1 F.4th 687, 707 (9th Cir. 2021), *cert. denied sub nom. Alphabet Inc. v. Rhode Island*, 212 L. Ed. 2d 233, 142 S. Ct. 1227 (2022) ("Allegations of suspicious stock sales or information from confidential witnesses are not needed where, as here, other allegations in the complaint raise a strong inference of scienter.").

Accordingly, the Court GRANTS the motion to dismiss claims regarding employee attrition as contained in the March and June 2022 risk disclosures, with leave to amend these allegations.

B. Data Security Incident

With regard to Okta's data security and the January 2022 incident, the complaint identifies five statements as false or misleading. *See* Opp'n at 12 (citing AC ¶¶ 143, 145, 159, 167–68). The Court finds these allegations fail to plausibly allege either falsity or scienter and so do not give rise to a claim under the PSLRA as currently stated in the complaint.

1. Okta's Commitment to Data Security

First, the statements Lead Plaintiff highlights regarding Okta's "commitment" to data security are not actionable. *See* AC ¶¶ 145 ("security is of the utmost importance to us"), 159 ("security is a mission-critical issue for Okta and for our customers").[8] Such statements "amount to vague and generalized corporate commitments, aspirations, or puffery that cannot support liability under Section 10(b) and Rule 10b-5(b)." *See In re Alphabet, Inc. Sec. Litig.*, 1 F.4th at 708 (in suit alleging cybersecurity vulnerability, statements about Google's commitment to privacy and data security "do not rise to the level of 'concrete description of the past and present' that affirmatively created a misleading impression of a 'state of affairs that differed in a material way from the one that actually existed.'") (citation omitted).

2. September 15, 2021 Conference Statement

Lead Plaintiff also challenges more specific representations that defendants made regarding data security. However, the complaint lacks particularized allegations showing that these statements were materially false when made. For instance, Lead Plaintiff challenges the following statement (in bold and italics) that Defendant McKinnon made at the Citi Global Technology Virtual Conference on September 15, 2021:

> So if you really get to this -- to get to this real Zero Trust capability, one of the things you have to do is you have to make sure that you

[8] Plaintiff concedes that it misattributed the statement quoted in paragraph 145 of the complaint, and that the statement was made by an Okta customer rather than an Okta VP. *See* Opp'n at 19 n.8.

> know, you have an inventory and you have an accurate representation of all the machines. So you have to have like a catalog of the machines. And then that's sometimes daunting enough. But then you have to make sure that you don't just -- you allow that machine to only do the minimum amount of things that it should be -- it should have to do.
>
> You can't just access anything on the network. You can't just potentially be a launching-off point for other attacks throughout your network. It has to be locked down to exactly what it has to be able to do. And to do that, you -- 9 times out of 10, you have to know the people that can do certain things from that machine. And that's the tricky part because a lot of these machines, they have a certain role that they do just in terms of processing kind of no user-related process and information around. ***But then they're left -- the administration accounts or the admin or the super user accounts are left open because it's easy for the engineers to drop in there and, like, do some admin things and maintain some network things.***
>
> And that's why -- that specific problem. Imagine the server in the server closet. You did a good job at Zero Trust. You took an inventory of the assets. You know this machine only should be able to access this other physical area of the network. You've really locked it down. But then you can log into that with an admin count and get anywhere.

AC ¶ 143. The complaint argues McKinnon's statements were false and misleading "because they omitted the material facts that Okta was not properly securing its administrative tools for monitoring customer tenants and that the Company failed to require its sub-processors to comply with the Company's fundamental security requirements." *Id.* ¶ 144. Yet plaintiff's assertion is not supported with specific factual allegations in the complaint.

The complaint relies on two confidential witnesses who stated that Okta could have done better in securing SuperUser access. CW6 was a Senior Solutions Engineer at Okta from February 2019 through December 2021 and who had SuperUser access. *Id.* ¶ 43. CW6 "suggest[ed] that the SuperUser tool should have been more closely guarded against hackers" and that "best practice" would have been to add additional safeguards such as requiring SuperUsers to access the tool only from a secure administrative station and not from their home laptops. *Id.* ¶ 100. CW7, an Okta Senior Solutions Engineer who stopped working for the company in March 2021, "advised that, in her opinion, Okta did not properly secure its administrative tools for controlling different cloud tenants[.]"[9] *Id.* ¶¶ 44, 102.

[9] The complaint does not state that CW7 had SuperUser access.

For several reasons, the accounts of CW6 and CW7 are not sufficient to support the assertion that Okta failed to require its sub-processors to comply with Okta's fundamental security requirements. For one, neither witness states what the complaint says they do—that Okta did not require its sub-processors to comply with Okta security requirements. Moreover, the opinion of CW7 is of little utility, where CW7 stopped working for Okta in March 2021, roughly ten months before the security incident occurred. *See id.* ¶ 44. In fact, CW6 herself explained that SuperUser access became more restrictive after June 2021. According to the complaint, CW6 recalled that "prior to June 2021, Okta had granted Solutions Engineers full SuperUser access, meaning they had full read and write access to customer tenants. However, CW6 recalled that Okta restricted Solutions Engineers' SuperUser access to read-only after June 2021 . . . ." *Id.* ¶ 147. Finally, it is unclear how the SuperUser allegations relate to the January 2022 incident, as nowhere does the complaint allege that the incident resulted from the breach of a SuperUser account. Plaintiff's brief argues that "the Company experienced a significant data security breach that was *caused by* Okta's failure to secure its administrative tools, such as the 'SuperUser' tool," but the complaint itself does not say this. *See* Opp'n at 7 (citing AC ¶¶ 98–104) (emphasis added). At the hearing, plaintiff's counsel conceded this, clarifying that plaintiff does not allege that SuperUser status was available to third party sub-processors such as the one whose account was compromised in January 2022. Rather, plaintiff's counsel stated that the SuperUser example shows that defendants were on notice that Okta was susceptible to a data breach.

More fundamentally, it is not clear from the excerpt quoted in the complaint exactly what Defendant McKinnon is talking about at the September 15, 2021 conference. He could be opining on ZeroTrust as a concept, talking about aspirations that Okta has, or describing a specific data security approach that Okta has already implemented. And as defendants point out, the statement does not even mention sub-processors. *See* Mot. at 11.

For all of these reasons, without more information the Court cannot find the complaint sufficiently alleges the statement McKinnon made on September 15, 2021, was false or misleading when made.

3. March 7, 2022 Risk Disclosure

Plaintiff also challenges the risk disclosure that Okta made in its Form 10-K, filed with the SEC on March 7, 2022. In its lengthy risk disclosures, Okta made the following statement related to data security: "***An application, data security or network incident may allow unauthorized access to our systems or data or our customers' data, disable access to our service, harm our reputation, create additional liability and adversely impact our financial results***." AC ¶ 159.

Plaintiff argues this statement was false and misleading because the risk warned of had already materialized: "Specifically, Okta had experienced the January 2022 Breach due to unsecured administrative tools used for monitoring cloud tenants and the failure to require sub-processors to comply with Okta's fundamental security requirements." *Id.* ¶ 160. In their motion to dismiss, defendants argue that not every security incident requires disclosure, and they dispute plaintiff's use of the term "breach." Instead, defendants state that the complaint provides "no specific factual allegations that Okta was aware of a breach—let alone a material one—by March 2022." Mot. at 13.

Setting aside for now the parties' dispute regarding falsity, the claim must be dismissed for lack of scienter. Defendants argue, and the Court agrees, that the complaint fails to allege sufficient facts showing what, if anything, the individual defendants knew about the January 2022 incident at the time Okta's Form 10-K was filed on March 7, 2022. None of the CWs allege that the individual defendants knew about the incident by March 7, 2022. What the complaint states is that the incident became public on March 21, 2022, when hackers posted screenshots "showing what they claimed was Okta's internal company environment." AC ¶ 105. On March 22, 2022, at 4:23 a.m., Defendant McKinnon posted on his Twitter account:

> In late January 2022, Okta detected an attempt to compromise the account of a third party customer support engineer working for one of our subprocessors. The matter was investigated and contained by the subprocessor. (1 of 2)
>
> We believe the screenshots shared online are connected to this January event. Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January. (2 of 2)

Id. ¶ 106. Later that same day, Okta's Chief Security Officer issued a blog post that, according to

plaintiff, "admitted that Okta first detected the January 2022 Breach in January." *Id.* ¶ 108. The complaint also alleges that "[o]n March 25, 2022, Okta acknowledged that it sat on this information for almost two months before stating, 'We want to acknowledge that we made a mistake.'" *Id.* ¶ 111.

The complaint thus provides no particularized facts to support the assertion that *the individual defendants* were aware of the January security incident by March 7, 2022. In its opposition, Lead Plaintiff argues that "CW3 explained during an All-Hands Meeting following the January 2022 Breach, [that] Defendants informed Okta employees that Okta 'quickly' knew the breach occurred and shut the compromised account down." Opp'n at 28. This misrepresents what is stated in the complaint. The complaint states, "According to CW3, the data breach that occurred in January 2022 and was disclosed in March 2022 was discussed at the first All-Hands Meeting *following the breach being publicized by news outlets*[,]" i.e., after March 22, 2022. *See* AC ¶ 113 (emphasis added). Thus, CW3's allegations do not show that the individual defendants knew of the incident prior to March 7, 2022. Nor do later statements from Okta's CEO that "Okta detected an attempt to compromise the account of a third party customer support engineer" in January 2022 raise a strong inference that defendants were aware of the event in January. The complaint neither paints a picture of "widespread deception" nor does it "sufficiently allege the individual Defendants acted with scienter." *See Oregon Pub. Emps. Ret. Fund*, 774 F.3d at 608.

Plaintiff also argues that it has adequately pled scienter under the core operations theory. Opp'n at 30, 32. "Proof under this theory is not easy. A plaintiff must produce either specific admissions by one or more corporate executives of detailed involvement in the minutia of a company's operations, such as data monitoring, . . .; or witness accounts demonstrating that executives had actual involvement in creating [the fraud]." *Police Ret. Sys. of St. Louis v. Intuitive Surgical, Inc.*, 759 F.3d 1051, 1062 (9th Cir. 2014) (citations omitted). Here, plaintiff has pled neither.

Finally, viewing the allegations of the complaint holistically, the Court still finds scienter lacking. Plaintiff essentially theorizes that because data security was the bread and butter of the company, it would be impossible for the individual defendants not to have known about the data

incident when it happened. When conducting a holistic review of the complaint, courts "must also 'take into account plausible opposing inferences' that could weigh against a finding of scienter. . . . Even if a set of allegations may create an inference of scienter greater than the sum of its parts, it must still be at least as compelling as an alternative innocent explanation." *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1006 (9th Cir. 2009) (quoting *Tellabs*, 551 U.S. at 323). Here, the Court cannot say that the allegations of the complaint are at least as compelling as the alternative innocent explanation, which is that a one-time attempted compromise of a third-party customer support engineer account that was "investigated and contained by the subprocessor" simply did not raise significant enough concerns when it happened to warrant alerting the company's CEO, CFO, and COO. *See* AC ¶ 106. This case is a far cry from *In re Alphabet, Inc. Securities Litigation*, on which plaintiff relies. That case involved an ongoing security glitch that the company learned had been leaving the private data of hundreds of thousands of users exposed for three years, and the complaint alleged that Google executives received an internal memo from legal and policy staff warning that disclosure of the security vulnerability would "almost guarantee[]" that Google's CEO would be brought to testify before Congress. 1 F.4th at 695–96. Here, the complaint lacks specific allegations regarding when the individual defendants learned of the security incident, nor does the incident on its face come close to the scale of the security concerns at issue in *Alphabet*.

4. Statements re: Customer Trust on June 8, 2022

Finally, plaintiff challenges statements that Defendant McKinnon made in a CNBC interview on June 8, 2022. Discussing the security incident that went public in March 2022, McKinnon stated,

> And anytime there's any kind of hack, whether it's to a third party or what any kind of talk of a breach, there's a lot of concerns in the [sic] in the customer base because this is about trust. So, the first thing we did is we had these conversations. We talked to over 1000 customers face to face over, [sic] over video and had these conversations. I personally talked [sic] over 400. ***And got a ton of feedback about what we could do better, how we could make sure that our support environment was not insecure, to make sure that we communicate better, to make sure that we are instill [sic] this trust. At the end of the [sic], I think we've been able to do that.***

. . .

> ***We're committed to making this a $4 billion a year company by fiscal year, fiscal year 26. So, that's, that's coming up quickly. So, we have to invest to grow to that scale and we've always done it with a balance of efficiency.*** We've always made sure that our, that our growth rate and our [sic] and our cash flow generation was balanced towards that goal. ***So, we think we're drawing the right balance to capture this market opportunity.*** And I think over time you're going to see a very highly scaled profitable company that's going to help customers and capitalize on this big market opportunity.

Id. ¶¶ 167–68 (underlined [sic]'s added by the Court).

Plaintiff alleges these statements were materially false and misleading when made "because Okta was actually losing sales as a direct result of the January 2022 Breach, which only compounded the severe problems the Company was having with the Auth0 integration." *Id.* ¶ 169. Plaintiff clarifies this argument in the opposition brief, charging that McKinnon's statement was false and misleading because "the January 2022 Breach had harmed Okta's reputation and sales, as customers no longer trusted the Company and were unwilling to increase their contracts or spend more money with Okta. [AC] ¶¶ 113-15." Opp'n at 23.

The complaint as it stands is not sufficiently particularized to show a false or misleading statement when made. For evidence that the company was losing sales, plaintiff relies on accounts from CW3, CW4, and CW8. CW3 reported "that the Company was saying that they were losing sales because of the breach," "that the breach did come up with every customer she spoke with," and that "the Company distributed 'talking points' to employees on how to 'downplay' the breach." AC ¶ 113. CW4 "recalled that prospective customers were deciding against doing deals with Okta after the breach." *Id.* ¶ 114. And CW8 "advised that Okta customers reacted negatively to the data breach that Okta disclosed in March 2022." *Id.* ¶ 115. Although "CW8 could not recall whether customers were canceling contracts outright[,]" CW8 did recall that the negative customer reaction "impacted her ability to meet quotas." *Id.* "CW8 could not quantify the amount of lost business, but she suggested it might have been 'tens of thousands of dollars' in lost business." *Id.*

These allegations lack particularity regarding how much sales Okta lost and when. With the exception of a single statement from CW8 estimating lost business in the tens of thousands of

dollars,[10] *see id.*, nowhere does the complaint identify with particularity which sales or how many were lost as a result of the data security incident. Moreover, both CW4 and CW8 left the company around the time of the data security disclosure. CW4 worked as an Account Executive at Okta "until the first quarter of fiscal 2023," which began February 1, 2022. *Id.* ¶ 41. CW8 worked as a Senior Account Executive "until spring 2022." *Id.* ¶ 45. Without more detail regarding when they departed, it is unclear that CW4 and CW8 would have been positioned to know the status of sales when McKinnon gave his interview in early June. And CW3, who stayed at the company until August 2022, does not allege having personally lost a single sale as a result of the data security incident. *See id.* ¶¶ 40, 113.

For these reasons, the complaint as it stands fails to show that the statements McKinnon made on June 8, 2022, were materially false or misleading when made.

C. Section 20(a)

A claim under Section 20(a), which provides for control person liability, "must demonstrate: (1) a primary violation of federal securities laws and (2) that the defendant exercised actual power or control over the primary violator." (internal quotation marks and citation omitted). A control person claim under Section 20(a) requires a predicate primary violation. *See Webb v. Solarcity Corp.*, 884 F.3d 844, 858 (9th Cir. 2018).

Where the Court has found that plaintiff has sufficiently stated a Section 10(b) claim (i.e., with regard to the March 2 and June 2, 2022 earnings call statements regarding the progress of the integration), the Court also finds that plaintiff has stated a claim under Section 20(a). For the remainder of the claims, where the Court has found no Section 10(b) violation is sufficiently alleged, the Court likewise finds plaintiff has failed to state a claim under Section 20(a).

II. Request for Judicial Notice

Along with their motion and reply briefs, defendants also filed a request for judicial notice.

[10] The Court assumes, though the complaint does not specify, that this figure references lost business on CW8's own sales accounts.

Dkt. Nos. 57, 58, 69. As a general rule, the Court may not consider any materials beyond the pleadings when ruling on a Rule 12(b)(6) motion. *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001). However, courts considering a motion to dismiss that is governed by the PSLRA may consider "documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs,* 551 U.S. at 322.

At this time, the Court declines to rule on defendants' request for judicial notice, as the Court did not rely on any of these documents in resolving the present motion.

CONCLUSION

For the foregoing reasons and for good cause shown, the Court hereby **GRANTS IN PART and DENIES IN PART** defendants' motion to dismiss, with leave to amend. The motion is GRANTED, except that the Court DENIES the motion as to omissions the individual defendants made regarding the Auth0 integration on the March 2 and June 2, 2022 earnings calls.

The second amended complaint shall be due no later than April 28, 2023.

When amending the complaint, Lead Plaintiff shall also attach a chart that lays out, concisely and with particularity, including paragraph citations to the second amended complaint: which statements Lead Plaintiff alleges were materially false or misleading; who made the statements; when the statements were made; and the facts (including dates) that Lead Plaintiff alleges render the statement false or misleading.

IT IS SO ORDERED.

Dated: March 31, 2023

SUSAN ILLSTON
United States District Judge